Claims:

1. A distributed storage system for storing at least one credential (46), provided by an issuing authority and relating to an identity (42, 44), the system comprising:

at least one unique identity (42, 44) having a local store (40), the store (40) of the at least one identity (42, 44) securely storing one or more credentials (46) relating to the owner of the identity (42, 44); and

a security certificate (66) provided at each identity (42, 44) for ensuring the authenticity of the one or more credentials (46), the security certificate (66) providing a secure reference to the issuer of the one or more credentials (46) that can be used in verifying the origin of each credential (46).

2. A system according to Claim 1, wherein the at least one identity (42, 44) comprises a hierarchical structure.

3. A system according to Claim 2, wherein the at least one identity (42, 44) comprises at least one role (48), the role (48) being a subset of the identity (42, 44) having its own credentials (46) within the identity (42, 44).

4. A system according to any of Claims 1 to 3, further comprising a host site (190), the host site (190) having a plurality of identities (42, 44) and associated stores (194, 196, 198).

5. A system according to Claim 4, wherein the host site (190) comprises a management module (200) for managing data access to and from the each of the identities (42, 44) and their associated stores (194, 196, 198).

6. A system according to Claim 4 or 5, wherein the host site (190) comprises a trusted financial institution's website (190).

7. A system according to Claim 1 or 4, wherein the identity (42, 44) or host site (190) comprises a website (80, 190).

8. A system according to Claim 7, wherein the identity further comprises a homepage (82) for providing general information regarding the identity (42, 44).

9. A system according to Claim 1, wherein the local store (40) of the identity (42, 44) comprises a portable mobile device which is connectable to a telecommunications network (84).

10. A system according to Claim 1, wherein the identity (42, 44) is arranged to store a private key (50) of the identity (42, 44) for encryption of the identity (42, 44).

11. A system according to Claim 10, wherein the identity (42, 44) is arranged to store a public key (52) of the identity (42, 44) for decryption of the identity (42, 44).

12. A system according to Claim 11, wherein the public key (52) of the identity (42, 44) is embedded within each credential (46) of the identity (42, 44).

13. A system according to Claim 1 or 11, wherein the identity (42, 44) is arranged to store a public key (58, 60, 62) of the authority (86) which has issued the one or more credentials (46) to the identity (42, 44).

14. A system according to Claim 13, wherein the public keys (52, 58, 60, 62) for each of the at least one role (48) and the identity (42, 44) are stored in the appropriate store (40) or identity (42, 44).

15. A system according to Claim 1, wherein at least some of the credentials (46) are arranged to be encrypted.

16. A system according to Claim 1, wherein the one or more credentials (46) each refer to the corresponding security certificate (66).

17. A system according to Claim 1, wherein the security certificate (66) comprises information describing the issuer (70), the identity to whom the certificate (66) has

been issued (72), a validity period (78) and a list (76) of credentials to which the certificate (66) relates.

18. A system according to Claim 1, wherein the certificate (66) is digitally signed using a private key and the certificate (66) contains the public key (58) for reading the digital signature (78).

19. A system according to Claim 1, wherein the identity further comprises a generator module (98, 200) for generating a certificate (66) regarding the identity (42, 44) for use in proxying credentials (46) to the store (88) of a different identity (42, 44).

20. A system according to Claim 1, wherein the identity (42, 44) further comprises a mailbox (90) for receiving messages from other identities (42, 44).

21. A system according to Claim 20, wherein the identity further comprises an authorisation function module (92) arranged to check that a request for access to the mailbox (90) has originated from an authorised identity (42, 44).

22. A method of storing credentials (46) relating to identities provided by an issuing authority in a distributed manner, the method comprising:

securely storing one or more credentials (46) relating to the owner of an identity (42, 44) in a local store (40) of the identity (42, 44); and

providing a security certificate (66) at the identity (42, 44) for ensuring the authenticity of the one or more credentials, the security certificate (66) providing a secure reference to the issuer of the one or more credentials (46) that can be used in verifying origin of each credential (46).

23. An identity (42, 44) of an entity for making available credentials (46) belonging to the entity to other entities, the identity (42,44) comprising:

a local store (40) arranged to securely hold one or more credentials (46) relating to the entity; and

a certificate processing module (98, 200) for reading and verifying received security certificates (66) and creating security certificates (170) for transmission, the security certificates (66, 170) providing a secure reference to the issuer of the one or more credentials (46) that can be used in verifying the origin of each credential (46).

5

24. A distributed storage system for storing a plurality of credentials (46), the system comprising a plurality of identities according to Claim 24.